

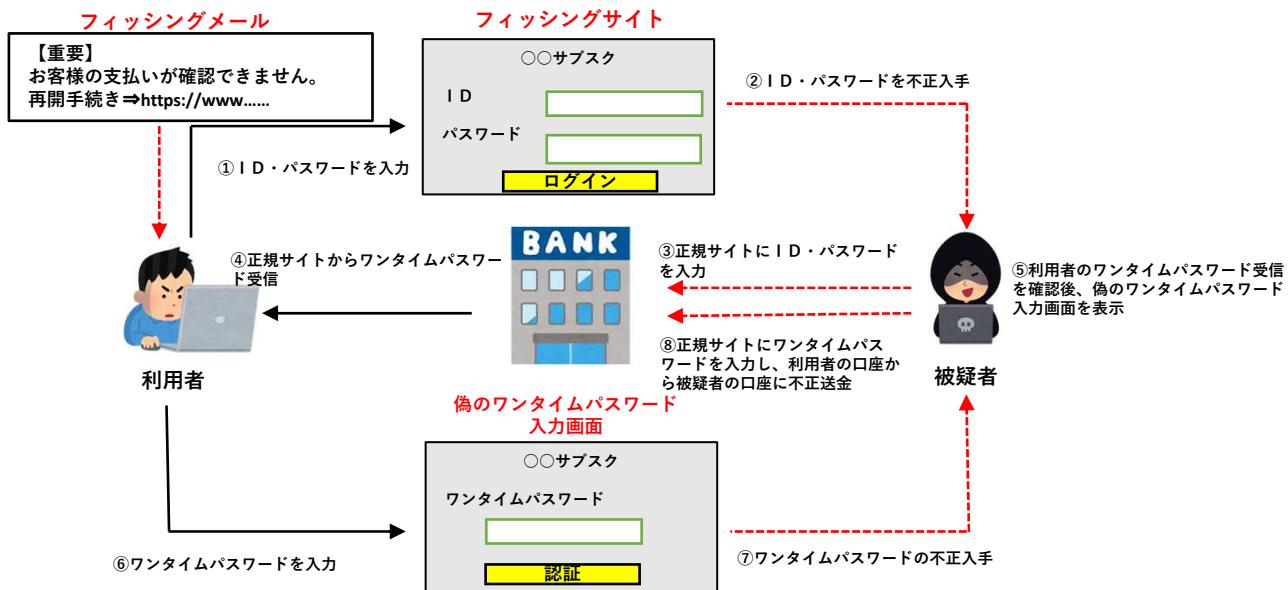
サイバーセキュリティ通信 【R7-19】

令和7年11月
大分県警察本部生活安全部
サイバー犯罪対策課

リアルタイムフィッシングに注意!!

リアルタイムフィッシングとは

実在する金融機関や企業等を装ったメールやSMSで偽のウェブサイトに誘導され、IDやパスワード、クレジットカード情報等をリアルタイムで窃取されるものです。IDやパスワード等を即座に正規サイトに入力され、ワンタイムパスワード等も盗まれてしまう手口を言います。



リアルタイムフィッシング被害に遭わないために

従来のフィッシング同様、基本的な対策が必要になります

- メールやSMSに記載されたリンク先にアクセスしない
⇒ 内容の確認は、公式サイトやアプリを利用する
- 送信元メールアドレスを確認する
- 生体認証を活用する（パスワードだけを利用しない）

【重要なお知らせ】や【お客様の口座に異常な取引を確認】等、不安を煽る文言に注意！！正しく安全にインターネットを便利に使いましょう！！



★詳しくは、警察庁HP**フィッシング対策**等を参照してください。

<https://www.npa.go.jp/bureau/cyber/index.html>



大分県警察
Oita Prefectural Police



Sect#バさん